White Paper
802.11 Wireless Local Area Network (WLAN)

Key Assumptions:

Security of wireless vs hardwire – In a hardwired environment, access to the network is limited by access to the physical environment (excluding Internet hacking). Wireless Local Area Networks are inherently insecure. Only by standards implementation, proper configuration and user education can risks be mitigated. WLAN transmissions can be intercepted a half-mile or more away from a transmitting site. Improperly configured devices or unauthorized wireless Access Points (APs) can significantly impede an organization's security posture.

Convenience vs. Security - Many organizations are considering obtaining wireless network devices as a convenient and cost effective alternative to hardwiring. Wireless also offers enhanced flexibility and mobility to the user. The devices are readily available in the marketplace, are inexpensive and relatively easy to install. However, many organizations and users do not consider the costs of security and administration of WLAN devices, or the risks to the organization if these activities are overlooked. An evaluation of WLANs must also include consideration of the impact these devices have on the ability of the organization's network management group to ensure systems availability, integrity, authentication, and confidentiality.

Devices shipped with wireless turned on by default. Many mobile computing devices, especially laptops and Personal Digital Assistants (PDAs), are commonly shipped with wireless access cards activated by default, in ad-hoc mode. If the devices are not specifically configured 1) for secure wireless access or 2) with wireless access disabled, utilization of the devices inside the physical boundaries of the organization creates an opportunity for unauthorized access to the network. Utilization in uncontrolled environments such as off-site meetings, hotels, airports etc… creates the opportunity for unauthorized access to the device and its data. Many users of these devices are unaware of the risks the devices present.

Rogue Access Points – Wireless APs are enabled by connecting wireless access devices to the network. Access devices installed without the knowledge and authorization of the organization's network management group are considered rogue access points. Rogue access points present a significant security and management risk to the organization.

Standards - The Wireless Fidelity (Wi-Fi) Alliance, which certifies 802.11 products, has adopted Safe Security Networks approach under the name Wi-Fi Protected Access (WPA). The recommended standard for procurement of WLAN devices is to obtain only those that are WPA certified. WPA is a data encryption method for 802.11 wireless

LANs. WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys. WPA will serve at least until the 802.11i standard is ratified (expected in 1st quarter, 2004) and implemented by the industry. WPA is expected to be viable through early 2005. Most existing Wi-Fi certified products can be upgraded to WPA standards through software upgrades. Implementation of 802.11i will require replacement of hardware. Organizations who have not yet implemented wireless solutions may choose to wait until 802.11i is available to avoid replacing hardware prior to the expiration of normal expected life cycle.

Configuration - Installing Wireless APs and devices out of the box without proper security configuration provides unrestricted access to the network All devices with wireless capability, whether or not they are intended to be used for wireless access, must be configured to by the network management and/or computer support group (or designee) in each organization. The devices must be configured, at a minimum by the following recommendations and requirements listed below.

Recommendations:

Organizations intending to utilize WLANs must adopt WPA as listed under "Standards" above.

WLANs should not be used to transmit highly confidential or classified data.

Access points for public use only (vendors on-site etc…) should either be segregated on a DMZ or provide access through a wireless security gateway (examples Bluesocket or Enterasys.)

Organizations should consider limiting off-hours traffic on WLANs, especially those accessed by the public.

WLAN security and configuration requirements

> WLAN technologies shall not be utilized for transmitting information unless the data is encrypted. WPA shall be utilized.
>
> User level authentication is required for all WLANs.
>
> If the WLAN system provides support for seamless roaming between access points (persistent sessions) then a session timeout capability must be provided and set at no more than 30 minutes.
>
> Connections to wireless APs for system management purposes shall only be via a console connection except where such connection is impractical. Hypertext Transfer Protocol (HTTP) and SNMP interfaces shall be turned off after initial configuration if not routinely used as part of the management process.

Reconfigure default settings on all wireless computing devices. Change all default passwords. Never the use built-in Windows XP wireless application. Use a secure 3rd party applet.

Disallow Ad-hoc networks: prohibit, by written policy, installation of rouge access points

Specific WLAN Configuration

With organization's CIO approval, 802.11 solutions will be used for unclassified data provided all of the following conditions are met:

- SSIDs (Service Set Identifier) will be changed from the manufacturer's default to a pseudo random number.
- The SSID broadcast mode will be disabled. WLANs that do not allow the SSID broadcast mode to be disabled will not be used.
- MAC (Media Access Control) address filtering will be turned on at each access point.
- If the WLAN system provides seamless roaming between access points (session persistence), the WLAN will provide a session timeout capability. The session timeout will be set for 30 minutes or less.
- PKI certificates will be used for identification and authentication of the user, if this capability is available and where the confidentiality of the data requires.
- The WLAN access point will be set to the lowest possible transmit power setting that will meet the required signal strength of the area serviced by the access point.
- File system encryption will be used on all WLAN client devices, if available.

The following additional WLAN security mechanisms are also required:

- Access points will be protected from attack as follows:

  - If a network layer or presentation/application layer security mechanism (e.g., IPSec, WTLS) is used to secure the WLAN system, IEEE 802.1x security, if available, will be implemented with a 128 bit encryption key to protect the access point from attack. Dynamic, per session, key change, and mutual authentication will be implemented. If IEEE 802.1x is not available on the WLAN system, WEP will be implemented on the system using a 128-bit encryption key.

  - Access points will be physically secured to prevent tampering/reprogramming (prevent unauthorized physical access).

  - HTTP and SNMP interfaces will be turned off after initial configuration.

  - Password access to the access point is turned on.

- Administrators responsible for wireless networks should actively pursue information concerning emerging exploits in the wireless environment.

Glossary

802.1x – A generic port based framework that allows the use of many types of authentication methods such as EAP-MD-5, EAP-TLS and EAP-TTLS. The protocol definition is EAP encapsulation over LANs (EAPOL).

802.11i - This supplemental draft standard is intended to improve WLAN security. It describes the encrypted transmission of data between systems of 802.11a and 802.11b WLANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). AES will require new hardware when it is completed in 2003.

AES – Advanced Encryption Standard **–** A 256 bit encryption standard most likely to replace WEP in the 802.11i group initiative.

AP – Access Point – Network equipment which in effect acts as a bridge between the wireless and wired network.

DMZ – De-militarized Zone

IEEE - The Institute of Electrical and Electronics Engineers, Inc., a non-profit, technical professional association.

IPSec - IP Security. A set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. An encryption method utilizing DES/3DES. It provides machine-level authentication and data encryption for VPN connections utilizing L2TP.

MAC – Media Access Control (address) – A 48-bit, six segment hexadecimal address to identify network equipment. The first three hextets are the manufacturer ID, and the last three are the unique ID of the piece of equipment.

PKI - Public Key Infrastructure

RADIUS – Remote Access Dial-In User Service – An industry standard mechanism for authenticating users over dial-up and VPN.

SNMP: Simple Network Management Protocol

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WLAN – Wireless Local Area Network

WEP - Wireless Equivalent Privacy/Protocol – A streaming ciphering algorithm based on RC4 developed by RSA Data Security, Inc. The RC4 encryption algorithm is secure, but its implementation in Wi-Fi is flawed regardless of key size. As the key size increases, it is only linearly (not exponentially) more difficult to crack.

WTLS - Wireless Transport Layer Security provides authentication, privacy and integrity for the Wireless Application Protocol. It is based on the widely used TLS v1.0.